II. SPECIFICATION AMENDMENTS

Please replace the Abstract as rewritten below:

Abstract

The invention relates to a method for transmitting data between a GRPS/EDGE radio access network and user equipment of a mobile system, and to user equipment using the method, and to GERAN. In the method, the data to be transmitted ~~in~~ is encrypted using an encryption algorithm at the transmitting end, the encrypted data is transmitted from the transmitting end to the receiving end, and the transmitted data is decrypted using an encryption algorithm at the receiving end. The used encryption algorithm is an encryption algorithm of the radio access network UTRAN employing the wideband code division multiple access method of the universal mobile telecommunications system, in which case the input parameters of agreed format required by the encryption algorithm are created on the basis of the operating parameters of the GPRS/EDGE radio access network GERAN.

Please replace the paragraph on page 1, lines 25-26 as rewritten below:

[0004] wherein C is the encrypted data, M is the encryption mask, P is the ~~unerypted~~ unencrypted data and $\oplus$ is the XOR operation.

Please replace the paragraph on page 2, lines 3-7 as rewritten below:

[0006] wherein P_1 and P_2 are ~~unerypted~~ unencrypted data with different content and C_1 and C_2 are encrypted data with different content. As can be seen, a possible eavesdropper can remove the mask by performing an XOR operation between the data having different content and encrypted using the same mask, thus breaking the encryption.

Please replace the paragraph beginning on page 3, line 31 through page 4, line 5 as rewritten below:

[0013] Specifications for third-generation mobile systems, such as UMTS, are being developed by 3GPP (Third Generation Partnership Project) ~~whose home pages at http://www.3gpp.org contain specifications related to the general structure and encryption of the system, which provide a good description enabling the use of the invention to a person skilled in the art~~. The 3GPP specifications which are related to encryption in particular are incorporated herein by reference:

- 3G TS 33.102 V3.2.0: Security Architecture

- 3G TS 25.301 V3.4.0: Radio Interface Protocol Architecture

- 3G TS 33.105 V3.3.0: Cryptographic Algorithm Requirements.

Please replace the paragraph on page 5, lines 1-7 as rewritten below:

[0017] UTRAN is made up of radio network subsystems RNS. The interface between RNSs is called Iur. RNS is made up of a radio network controller RNC and one or more nodes B. The interface between RNC and B is called Iub. The coverage area, i.e. cell, of a node B is marked C in Figure ~~1B~~ 1A. RNS can also be called by its more traditional name, base station system (BSS). The network part of the radio system thus comprises a radio access network UTRAN and a core network CN.

Please replace the paragraph on page 12, lines 29-30 as rewritten below:

[0050] The ~~uncrypted~~ unencrypted data 414 is combined by an XOR operation 416 with the encryption mask ~~416~~ 412 to obtain the encrypted data 418.

Please replace the paragraph on page 12, lines 31-34 as rewritten below:

[0051] At the receiving end, the encryption is removed using a similar operation as in the transmitting end, i.e. the encryption mask 412 is combined by an XOR operation 416 with the received encrypted data 418 to obtain the original ~~uncrypted~~ unencrypted data 414.

Please replace the paragraph beginning on page 12, line 35 to page 13, line 14 as rewritten below:

[0052] The transmitting and receiving ends must be synchronized with each other in the sense that the parameters 402, 404, 406, 408, 410 of the encryption algorithm 400 used to encrypt certain data 414 must also be used to decrypt the encrypted data 418 corresponding to said ~~uncrypted~~ unencrypted data 414. Implementing this may require signaling between the transmitting end and the receiving end. This or data modulation and channel coding are not described in more detail herein, because they are not essential for the invention and are known actions to a person skilled in the art. It is enough to note that the transmitting end comprises means 400, 416 for encrypting data to be transmitted to the receiving end using an encryption algorithm 400, and the receiving end correspondingly comprises means 400, 416 for decrypting data received from the transmitting end using the encryption algorithm 400. Because the connection between GERAN and the user equipment is bi-directional, both can serve as transmitting and receiving ends. Thus, both GERAN and the user equipment comprise both the encryption means and the decryption means.

Please replace the paragraph on page 15, lines 8-15 as rewritten below:

[0059] The UTRAN counter parameter ~~410~~ 402 is a 32-bit counter changing with time and formed by the hyper frame number and RLC sequence number, for instance. In the original GSM system, a 22-bit TDMA frame number is used as the counter parameter. This

means that the counter parameter reaches its maximum value already after approximately 3.5 hours of encryption. When the counter parameter starts again, the mask begins to get the same values again and the encryption can be broken unless a new encryption key is taken into use.

Please replace the paragraph on page 15, lines 16-29 as rewritten below:

[0060] The counter parameter ~~410~~ 402 cannot as such be used in GERAN, but its contents must be changed while the length remains at 32 bits. When using the RLC protocol, the counter parameter ~~410~~ 402 is formed by the RLC sequence number, a symbol which defines whether the data to be encrypted is data of the second layer signaling plane or other data, and the hyper frame number. The length of the hyper frame number can be 24 bits, in which case the length of the RLC sequence number is 7 bits, or the hyper frame number can be 20 bits long, in which case the RLC sequence number is 11 bits long. The 1-bit symbol which defines whether the data to be encrypted is data of the second layer signaling plane or other data obtains in this case the value 1, when the data to be encrypted is other data than data of the second layer signaling plane. In practice, when using the RLC protocol, the effective length of the counter parameter becomes 31 bits, while the 1-bit symbol is constant.

Please replace the paragraph beginning on page 15, line 30 through page 16, line 5 as rewritten below:

[0061] When using the MAC protocol, the counter parameter ~~410~~ 402 is formed by an extended TDMA frame number, a time-slot number and a symbol defining whether the data to be encrypted is data of the second layer signaling plane or other data. The length of the TDMA frame number is thus extended to 28 bits. The 1-bit symbol which defines whether the data to be encrypted is data of the second layer signaling plane or other data obtains in this case the value 1, when the data to be encrypted is other data than data of the second layer signaling plane. The time slot number can be constant, if only one time slot is used. In practice, when using the MAC protocol, the effective length of the counter parameter becomes 28 bits, while the 1-bit symbol and the time slot number are constant. This is 64 times more than the cycle of the present GSM counter parameter, and thus sufficient in practice.

Please replace the paragraph on page 17, lines 3-11 as rewritten below:

[0067] The counter parameter ~~410~~ 402 is formed for the second layer signaling plane data in the same way as for other data when using the MAC protocol, i.e. the counter parameter ~~410~~ 402 is formed by an extended TDMA frame number, a time slot number and a symbol which defines whether the data to be encrypted is data of the second layer signaling plane or other data. The 1-bit symbol which defines whether the data to be encrypted is data of the second layer signaling plane or other data obtains in this case

the value 0, when the data to be encrypted is data of the second layer signaling plane. The entire MAC block is encrypted.

Please replace the paragraph beginning on page 18, line 31 through page 19, line 18 as rewritten below:

[0072] In a preferred embodiment, when the connection of the user equipment UE changes between the GPRS/EDGE radio access network GERAN and the radio access network UTRAN employing wideband code division multiple access method, information on the last used extended TDMA frame number or hyper frame number is provided to the new radio access network, and the same encryption key input parameter 408 as in the old radio access network is used as the encryption key input parameter 408 of the encryption algorithm 400 in the new radio access network. This way, it is possible to avoid the use of the same mask 412 for ~~unerypted~~ unencrypted data 414 with different content. Without this procedure, it would be necessary to always perform the signaling required by the initiation of a new encryption key between the user equipment UE and the GPRS/EDGE radio access network GERAN when the connection changes, due to handover, for instance. In principle, this procedure can be implemented in two ways, either so that the user equipment comprises means 190, 192, 194 for providing information on the last used extended TDMA frame number or hyper frame number to the new radio access network when the connection of the user equipment UE changes between the GPRS/EDGE radio access network GERAN and the radio access network UTRAN employing wideband code division multiple access method, or so that the GPRS/EDGE radio access network GERAN comprises means 180 for receiving information on the last used extended TDMA frame number or hyper frame number to the user equipment UE when the connection of the

user equipment UE changes between the GPRS/EDGE radio access network GERAN and the radio access network UTRAN employing wideband code division multiple access method.

Please replace the paragraph on page 19, lines 19-33 as rewritten below:

[0073] The described procedures are preferably implemented in such a manner that the information to be stored or provided comprises a certain number of the most significant bits, and before the information is used in the new radio connection or radio access network, the value of the number formed by the most significant bits is increased by one. This way, it is possible to avoid the use of the same encryption mask 412 twice for ~~unerypted~~ unencrypted data 414 with different content. This can be implemented so that either the user equipment UE or the GPRS/EDGE radio access network GERAN comprises means 402 for increasing by one the value of the number formed by said most significant bits before the information is used in a new connection or in the new radio access network. For instance, when moving from GERAN to UTRAN, 20 most significant bits could be stored and when moving from UTRAN to GERAN, 17 most significant bits could be stored. This way, the differences between the less significant parts remain unimportant, and it is possible to ensure that the same encryption mask 412 is not used twice.